REMARKS

Applicant respectfully requests reconsideration of the subject application as amended herein and submits that no new matter has been added thereby.

Please charge any shortages and credit any overages to our Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 3/25/02

Justin M. Dillon
Reg. No. 42,486

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(512) 330-0844

MARKED-UP VERSION SHOWING CHANGES MADE

IN THE SPECIFICATION

Please replace paragraph 3 beginning on page 2 with the following rewritten paragraph:

-- Conventional modular multipliers often include a linear systolic array or "chain" of processing elements (PEs) implemented in hardware such as an application-specific integrated circuit (ASIC) or a programmable logic device such **as** a field programmable gate array (FPGA) [**where**]. In conventional modular multipliers, a given processing element performs a portion of a modular multiplication operation by processing data and then passing it to its neighboring or adjacent PEs in a given clock cycle. In the next clock cycle, the original processing element remains idle while the neighboring processing elements process the received data and pass the processed data back, after which the original processing element may spend another cycle computing. Thus, in most conventional modular multipliers, each processing element does useful work every other clock cycle and is idle the remainder of the time. In one traditional modular multiplier, these idle cycles are used to concurrently perform an additional limited modular multiplication operation where two of three operands, B and M, must be the same.--

Please replace paragraph 30 beginning on page 11 with the following rewritten paragraph:

--In the embodiment illustrated in **Figure 2**, rather than utilize the first and second independent computation channels to perform two distinct modular multiplication operations, the computation channels are combined to form a single "virtual" computation chain according to the present invention by feeding the end of the linear systolic array of processing elements back into the beginning of the array. The second computation channel is consequently utilized as a continuation of the first, effectively doubling the length of the linear systolic array while sacrificing one of the available multiplication channels. It should be appreciated however that in alternative embodiments of the invention the resulting effective linear systolic array length may be greater than or less than twice the original length. For example, embodiments of the invention may be implemented in which a linear systolic array having more than two independent computation channels is utilized resulting in a longer effective array length. Similarly, an embodiment in which not all processing elements of a linear systolic array are utilized or included within the provided feedback loop **<u>may be implemented,</u>** resulting in a shorter effective array length.--

Please replace paragraph 33 beginning on page 12 with the following rewritten paragraph:

--Consequently, the static fed-back modular multiplier embodiment illustrated in **Figure 2** may be utilized to perform an n-bit modular multiplication operation using a linear systolic array having a number of processing elements ordinarily sufficient to perform an n/2-bit modular multiplication operation. For purposes of this description therefore, the processing elements **<u>of</u>** the illustrated array or chain will be referred to by number from 0 to [**the**] N/2 + 2 from left to right starting with the first processing element, where N is equal to the number of digits within the operands processed in the modular multiplication. So for example, a 1024-bit modular multiplication operation, ordinarily requiring 259 4-bit processing elements plus end logic (i.e. 1024 / 4 = N = 256 + 3 additional PEs = 259) would instead require 131 4-bit processing elements (N = 256 / 2 = 128 + 3 = 131). In one embodiment of the present invention, a restriction exists requiring that the number of processing elements in the fed-back chain is odd so that data fed back from the end of the first computation channel arrives at the beginning of the second computation channel and hits otherwise idle computation cycles of the processing elements of the array and not busy cycles. In an alternative embodiment where an even number of processing elements is required in an array, [**a**] **<u>an</u>** odd number of additional processing elements (e.g. one additional processing element) may be included within the array but outside of the feedback loop itself. The additional processing element(s) may be incorporated into the end logic or otherwise placed to the left of the feedback loop or alternatively to the right of the feedback loop, prior to second multiplexer 208.--

<u>IN THE CLAIMS</u>

Please amend claims 1, 9, and 17 as indicated and add claims 31-33:

1. (Amended) An apparatus comprising:

a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel; **and**

a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.

9. (Amended) A processor comprising:

a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel; **and**

a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.

17. (Amended) A system comprising:

a memory to store data and instructions;

a first processor coupled to said memory to process data and execute instructions; [**and**]

a second processor coupled to said memory, said second processor comprising:

a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel; **and**

a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.

31. (New) A method comprising:

receiving a data value at a first end of a systolic array multiplier from a second end of the systolic array multiplier and receiving a data value at the second end from the first end.

32. (New) The method of claim 31, wherein receiving a data value at a first end of a systolic array multiplier from a second end of the systolic array multiplier comprises:

receiving a data value from a second end of the systolic array multiplier at a first input of a multiplexer;

receiving a channel data input signal at a second input of the multiplexer; and

providing either the data value from the second end of the systolic array multiplier or the channel data input signal to the first end of a systolic array multiplier via an output of the multiplexer.

33. (New) The method of claim 31, further comprising:

processing data in processing elements which operate on a given problem during alternating cycles of a clock signal.